(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 28 936 A 1**

(51) Int. Cl.[6]:
G 06 F 3/06
G 06 F 12/14
H 04 L 9/20

(21) Aktenzeichen: 198 28 936.7
(22) Anmeldetag: 29. 6. 98
(43) Offenlegungstag: 2. 12. 99

DE 198 28 936 A 1

(66) Innere Priorität:
198 24 163. 1 29. 05. 98

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Sedlak, Holger, 85658 Egmating, DE; Smola, Michael, 80636 München, DE; Wallstab, Stefan, 81739 München, DE; Söhne, Peter, Dr.rer.nat., 85244 Röhrmoos, DE

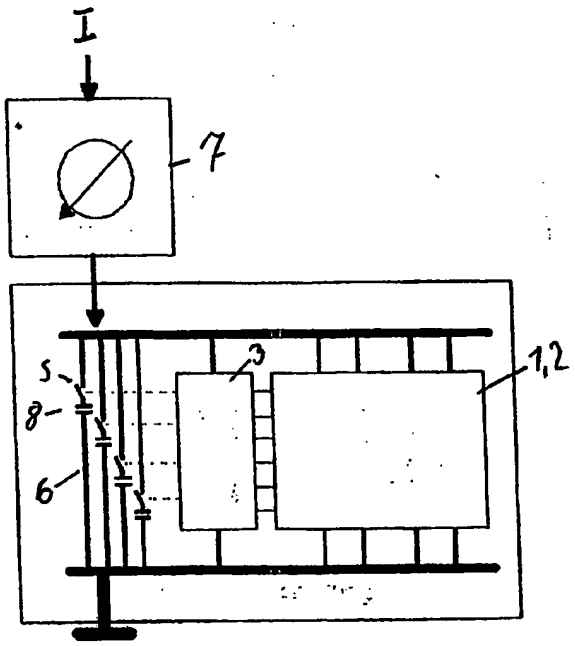
(56) Entgegenhaltungen:
DE 1 96 42 560 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren und Vorrichtung zum Verarbeiten von Daten

(57) Es ist ein Verfahren zum Verschlüsseln und/oder Entschlüsseln von Daten, bei dem die Daten für ein Verschlüsseln oder Entschlüsseln in einem Verschlüsselungs- oder Entschlüsselungsschritt vorgesehen werden, der aus mehreren alternativen gleichwertigen Verschlüsselungs- oder Entschlüsselungsschritten ausgewählt ist, und/oder aus mehreren sequentiell abzuarbeitenden Verschlüsselungs- oder Entschlüsselungsteilschritten besteht, wobei der ausgewählte Verschlüsselungs- oder Entschlüsselungsschritt zufällig ausgewählt ist und/oder die Verschlüsselungs- oder Entschlüsselungsschritte zufällig verändert sind, vorgesehen.



DE 198 28 936 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren bzw. eine Vorrichtung zum Verarbeiten von Daten. Im Rahmen üblicher Datenverarbeitung werden heut zutage zunehmend Sicherheitsaspekte relevant, da zunehmend versucht wird, unerlaubt Daten aus Datenverarbeitungsanlagen zu erhalten. Um die zu verhindern werden zunehmend kryptographische Verfahren angewandt, bei denen zu schützende Daten verschlüsselt werden. Hierzu wird unter anderem beispielsweise das "Public-Key-Verfahren" verwendet, bei dem jeder Teilnehmer eines Systems ein Schlüsselpaar besitzt, das aus einem geheimen Schlüsselteil und einem öffentlichen Schlüsselteil besteht. Die Sicherheit der Teilnehmer beruht nun darauf, daß der geheime Schlüsselteil Unbefugten nicht bekannt ist. Die Ausführung eines derartigen Verfahrens geschieht häufig in einer besonders gesicherten Komponente, wie beispielsweise einer Chipkarte aber auch in einem einmal in ein Gerät eingesetzten elektronischen Schaltkreis – auch als IC bekannt –, in denen dann das Verfahren selbst realisiert ist. Somit braucht der geheime Teil des Schlüssels diese gesicherte Komponente nicht zu verlassen.

Neuerdings sind jedoch Angriffe bekannt geworden, bei denen versucht wird, den Schlüssel in der gesicherten Komponente auszuspähen. Dies soll beispielsweise durch Messung des Stromverbrauchs der gesicherten Komponente ermöglicht werden. Durch das häufig wiederholte Beobachten des Stromverlaufs und bei dem Bekanntsein wie der Verschlüsselungsvorgang durchgeführt ist, ist es schließlich möglich, Rückschlüsse auf den Schlüssel zu ziehen.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zum Verschlüsseln bzw. eine Vorrichtung vorzusehen, bei der eine erhöhte Sicherheit vor dem Ausspähen eines geheimen Schlüsselwortes gegeben ist.

Diese Aufgabe wird erfindungsgemäß mit den Maßnahmen bzw. Mitteln gemäß Patentanspruch 1 bzw. Patentanspruch 3 gelöst.

Dadurch, daß Verschlüsselungs- bzw. Entschlüsselungsverfahren so gesteuert bzw. Operationen begleitend zu diesem Verfahren gesteuert werden, daß sich auch bei einer häufig wiederholten Messung von von außen zugänglichen Parametern, wie beispielsweise dem Stromverbrauch, keine Rückschlüsse auf den verwendeten Schlüssel ziehen lassen.

Weitere vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben. Nachfolgend wird die Erfindung unter Bezugnahme auf die Zeichnung anhand von Ausführungsbeispielen erläutert.

Hierbei zeigen:

Fig. 1 ein erstes Ausführungsbeispiel einer erfindungsgemäßen Vorrichtung,

Fig. 2 ein zweites Ausführungsbeispiel einer erfindungsgemäßen Vorrichtung, anhand der auch das erfindungsgemäße Verfahren erläutert wird und

Fig. 3 ein drittes Ausführungsbeispiel.

Mit **1**, **2** ist eine zu schützende Schaltung, die beispielsweise aus einem Mikrocontroler **2** und einem Rechenwerk **1** besteht, bezeichnet. Der Mikrocontroler **2** steuert dabei das Rechenwerk **1**, in dem beispielsweise ein Verschlüsselungsvorgang durchgeführt wird. Dieser zu schützenden Anordnung wird nunmehr ein Strom I zugeführt, der mittels einer Meßeinrichtung **7** detektierbar ist, wodurch Rückschlüsse auf die Vorgänge in der zu schützenden Schaltung **1**, **2** gezogen werden sollen. Es ist nunmehr eine zusätzliche Schaltungseinrichtung **6** vorgesehen, die über einen Zufallsgenerator **3** gesteuert wird. Dieser Zufallsgenerator kann beispielsweise als ein Sequenzgenerator in Form eines linear rückgekoppelten Schieberegisters ausgeführt sein, welches mit einem Startwert geladen, eine pseudozufällige Folge – Nullen und Einsen – erzeugt. Hierbei kann der Startwert entweder zufällig erzeugt sein oder von der Steuereinrichtung beispielsweise auf Basis des Schlüsselwortes generiert werden, auch ist eine Kombination beider Möglichkeiten denkbar. Die somit vom Zufallsgenerator erzeugte Sequenz steuert nunmehr Schalter S in der zusätzlichen Schaltungseinrichtung **6**, so daß Kondensatoren, die mit den Schaltern S in Reihe liegen, entsprechend der jeweils gerade erzeugten Zufallsfolge geladen werden. Auf diese Weise wird der Stromverbrauch der zu schützenden Schaltung **1**, **2** durch die zusätzliche Schaltungseinrichtung **6**, nämlich dem Ladestrom der Kondensatoren, verschleiert. Um den Gesamtstromverbrauch dieser Einrichtung zu minimieren, ist es nicht notwendig, daß die zusätzliche Schaltungseinrichtung **6** fortwährend einen Beitrag zum Stromverbrauch liefert. Sie kann vielmehr darauf beschränkt werden, nur in der Zeit während des Verschlüsselns bzw. Entschlüsselns zu arbeiten.

Fig. 2 zeigt ein weiteres erfindungsgemäßes Ausführungsbeispiel. Hierbei liegt das Rechenwerk **1** und die Steuerungseinrichtung **2**, der Zufallsgenerator **3** und eine Speichereinrichtung **5** an einem gemeinsamen Bus **4**, der von extern mittels einer Schnittstelle **9** zugänglich ist. Über die Schnittstelle **9** werden beispielsweise zu verschlüsselnde bzw. zu entschlüsselnde Daten zugeführt. In der Speichervorrichtung **5** ist ein geheimes Schlüsselwort gespeichert, das gesteuert von der Steuereinrichtung **2** dem Rechenwerk **1** zugeführt wird, um die über die Schnittstelle **9** vom Datenbus zugeführten Daten zu verschlüsseln bzw. zu entschlüsseln. Der Zufallsgenerator **3** erzeugt nunmehr eine Zufallszahl, die der Steuereinrichtung **2** zugeführt wird, die nunmehr auf Grundlage dieser Zufallszahl das Rechenwerk **1** steuert. Hierbei sind nunmehr zwei Möglichkeiten denkbar.

Das Rechenwerk **1** wird auf Grundlage der Zufallszahl durch die Steuereinrichtung **2** so gesteuert, daß der Verschlüsselungs- oder Entschlüsselungsalgorithmus der jeweiligen Zufallszahl entsprechend moduliert wird. Das bedeutet, es erfolgen somit im Verschlüsselungs- bzw. Entschlüsselungsalgorithmus Rechenoperationen, die ohne abschließende Auswirkung auf die Verschlüsselung bzw. Entschlüsselung, mit zufälligen Werten arbeiten.

Nachfolgend werden Beispiele für die Variationen des Verschlüsselungs- bzw. Entschlüsselungsalgorithmus beschrieben.

Ein bekanntes Verfahren ist das sogenannte RSA-Verfahren. Es arbeitet in der Gruppe teile fremder Restklassen modulo N und setzt die Exponentiationen aus Multiplikationen modulo N zusammen. Die Varianten dieser Protokolle für elliptische Kurven modulo p besitzen aus modularen Additionen und Multiplikationen zusammengesetzte Grundoperationen, sogenannte Additionen und Verdoppelungen in der Punktgruppe der elliptischen Kurven, die ihrerseits zur Exponentiation zusammengesetzt werden. Die dritte große Gruppe besteht aus elliptischen Kurven über endlichen Körpern, deren Elementezahlen eine Primzahlpotenz, die häufig eine Potenz von 2 ist. Diese Strukturen werden gemeinhin als $GF(p^n)$ bezeichnet. Die Basisarithmetik in diesen Körpern kann durchgeführt werden, indem man die Körperelemente als Polynome mit Koeffizienten aus dem Grundkörper GF(p) oder einem geeigneten Zwischenkörper darstellt, die durch Multiplikationen modulo einem festen Körperpolynom miteinander verknüpft sowie koeffizientenweise addiert werden. In diesem Sinne lassen sich Operationen in $GF(p^n)$ bzw. in elliptischen Kurven über diesen Körper als modulare Rechenoperation auffassen. Dabei sind die nachfolgenden drei, dem erfindungsgemäßen Verfahren entsprechende Variationsmöglichkeiten möglich.

a) Der Modul N wird durch $r \cdot N$ ersetzt, wobei r eine von O verschiedene Zufallszahl ist. Im $GF(p^n)$-Fall wird das Körperpolynom durch sein Produkt mit einem zufällig gewählten von 0 verschiedenen Polynom ersetzt. Dieser Schritt ist vor Eintritt in die Rechnung oder einem Teilschritt durchzuführen und nachfolgend durch eine Reduktion des Ergebnisses bzw. Teilergebnis modulo N zu kompensieren.

b) Ein Eingangsparameter X einer modularen Rechenoperation wird durch den Wert $X + s \cdot N$ ersetzt, wobei s eine Zufallszahl ist. Dies kann in verschiedenen Rechenschritten durchgeführt werden. Auch eine entsprechende Veränderung mehrerer Eingangsparameter der selben Operation ist möglich.

c) Die Exponenten E werden durch $E + t \cdot q$ ersetzt, wobei t eine Zufallszahl und q die sogenannte Ordnung der Basis der auszuführenden Exponentiation, oder ein geeignetes Vielfaches davon, ist. Potentielle Werte von q lassen sich häufig aus den Systemparametern ableiten. So kann man für die Exponentiation modulo N $q=\varphi(N)$ und für elektrische Kurven g als die Anzahl der Punkte dieser Kurve wählen, wobei häufig noch bessere Wahlmöglichkeiten gegeben sind.

Eine weitere Möglichkeit besteht darin, daß alternative, gleichwertige Verschlüsselungs- bzw. Entschlüsselungsalgorithmen im Rechenwerk **1** durchführbar sind, die gemäß der zugeführten Zufallszahl zufällig ausgewählt werden.

Bei der zuvor beschriebenen Modulation des Verschlüsselungs- bzw. Entschlüsselungsalgorithmus wird nicht nur der Stromverbrauch der Anordnung durch die Zufallszahl verändert, sondern ebenfalls die benötigte Rechenzeit. Auch diese kann als Meßgröße Rückschlüsse auf den Geheimschlüssel geben. Gleiches gilt für die zufallsgesteuerte Auswahl der äquivalenten Rechenoperationen.

Eine dritte Möglichkeit ist darin zu sehen, daß ähnlich dem Ausführungsbeispiel nach **Fig.** 1 eine zusätzliche Schaltungseinheit **6** vorgesehen ist (gestrichelt dargestellt), die ebenfalls mit der Zuführeinrichtung **4** verbunden ist. Die Steuereinrichtung **2** steuert nunmehr die zusätzliche Schaltungseinrichtung **6** gemäß einer vom Zufallsgenerator **3** über die Zuführeinrichtung **4** zugeführten Zufallszahl. Eine Analyse des Stromverbrauchs der dargestellten Gesamtanordnung ist somit nicht durch den Betrieb im Rechenwerk **1** allein bestimmt sondern ebenfalls durch einen zufällig gesteuerten Stromverbrauch der zusätzlichen Schaltungseinheit.

Zusätzlich sei darauf hingewiesen, daß auch die Kombination von Modulation des jeweiligen Algorithmus mit einer zusätzlichen Schaltungseinheit **6** im "Dummy-Betrieb" sinnvoll ist.

Fig. 3 zeigt ein drittes erfindungsgemäßes Ausführungsbeispiel. Hierbei wird der Steuereinrichtung **2**, in Form einer CPU über Datenanschluß D Daten zugeführt. Gleichzeitig wird der "Wait-State-Anschluß" WS mit einem Zufallsgenerator **3** verbunden. Dieser Zufallsgenerator **3** erzeugt nunmehr in zufälliger Folge "Einsen" "Nullen". Entsprechend der Programmierung wird nunmehr immer dann wenn eine "1" oder "0" am Eingang anliegt, der Betrieb der CPU gestoppt oder wieder aufgenommen. Dies führt dazu, daß der Betrieb der CPU zwar noch synchron zu einem nicht dargestellten Taktgenerator arbeitet, jedoch keine einheitlichen Verarbeitungszyklen mehr aufweist. Da auf diese Weise kein fester einheitlicher Rahmen mehr vorliegt, sind durch Beobachtung der CPU deren Arbeitsvorgänge nicht mehr ohne weiteres nachvollziehbar und nur sehr erschwert analysierbar. Dies bedeutet, daß die in der CPU abzuarbeitenden Vorgänge "verrauscht" sind. Um die Randhabbarkeit einer solchen Anordnung zu steigern, kann der Zufallsgenerator **3** so programmiert werden, daß festlegbar ist, in welchem zeitlichen Rahmen eine Verarbeitung maximal abläuft. Dies ist unter anderem dafür notwendig, um festzustellen, ob das System insgesamt ausgefallen ist.

Es erscheint besonders sinnvoll eine Anordnung gemäß **Fig.** 3 mit einer Anordnung gemäß **Fig.** 1 oder 2 oder mit beiden zu kombinieren um somit beispielsweise die Analyse der Bearbeitung eines Gesamtsystems zu erschweren.

Patentansprüche

1. Datenverarbeitungsverfahren, bei dem in einer Verarbeitungseinheit (**1**, **2**) über eine Datenleitung zugeführte Daten verarbeitet werden, ein Zusatzsignal der Verarbeitungseinheit zugeführt wird, und bei dem die Verarbeitung in Abhängigkeit vom Zusatzsignal erfolgt.
2. Datenverarbeitungsverfahren nach Anspruch 1, bei dem das Zusatzsignal von einem Zufallszahlgenerator gesteuert ist.
3. Datenverarbeitungsverfahren nach Anspruch 2, bei dem an einer geeigneten Stelle ein Operand mit einer Zufallszahl beaufschlagt ist und an einer weiteren geeigneten Stelle ein entsprechender Kompensationsoperand mit der gleichen Zufallszahl beaufschlagt ist.
4. Datenverarbeitungsverfahren nach Anspruch 2, bei dem die Verarbeitung der Daten aus mehreren Einzelschritten zusammengesetzt ist, die aus mehreren Alternativen gleichwertigen Einzelschritten ausgewählt sind, und/oder aus mehreren sequentiell abzuarbeitenden veränderbaren Einzelschritten besteht, wobei die Auswahl und/oder die Veränderung auf Grundlage des Zusatzsignals erfolgt.
5. Vorrichtung zum Durchführen des Verfahrens nach Anspruch 1, mit einer Recheneinrichtung (**1**), der Daten mittels einer Zuführvorrichtung (**4**) zugeführt werden, und einem Zufallsgenerator (**3**), und einer Steuervorrichtung (**2**), die die Recheneinrichtung steuert, wobei ein Ausgangssignal des Zufallsgenerators (**3**) die Steuereinrichtung (**2**) und/oder und die Recheneinrichtung (**2**) beeinflußt.
6. Vorrichtung nach Anspruch 5, bei der mit der Steuereinrichtung (**2**) eine Hilfsschaltung (**6**) verbunden ist, die von der Steuereinrichtung (**2**) auf Basis des von dem Zufallsgenerator (**3**) zugeführten Ausgangssignal gesteuert wird.

Hierzu 3 Seite(n) Zeichnungen

Nummer: DE 198 28 936 A1
Int. Cl.[6]: G 06 F 3/06
Offenlegungstag: 2. Dezember 1999

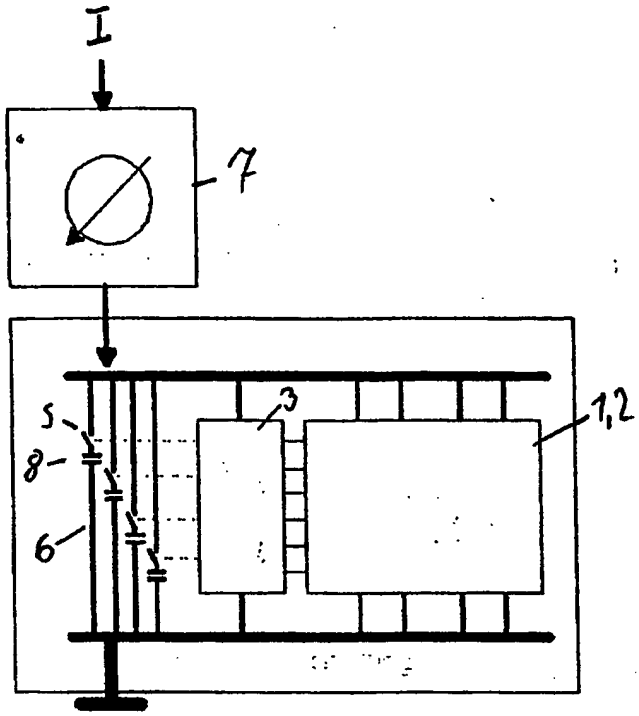


Fig. 1

Nummer: DE 198 28 936 A1
Int. Cl.[6]: G 06 F 3/06
Offenlegungstag: 2. Dezember 1999

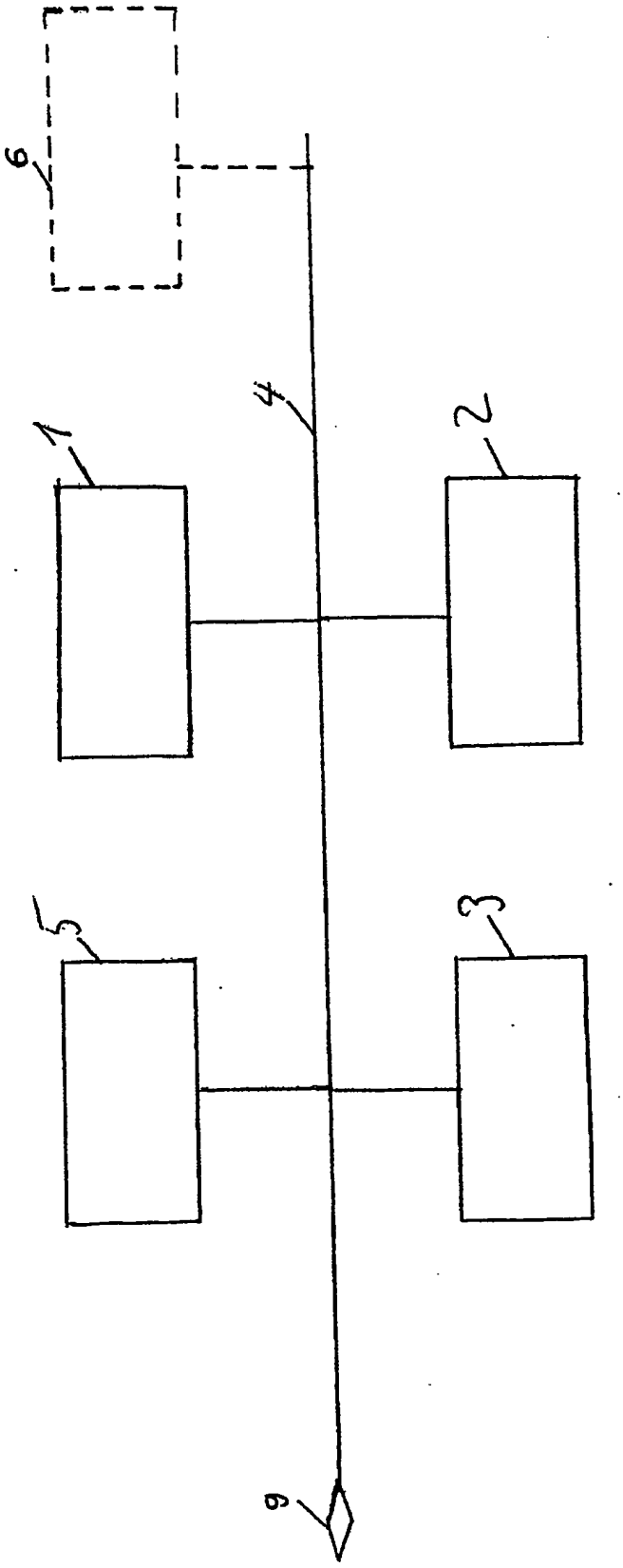


Fig. 2

Nummer: DE 198 28 936 A1
Int. Cl.[6]: G 06 F 3/06
Offenlegungstag: 2. Dezember 1999

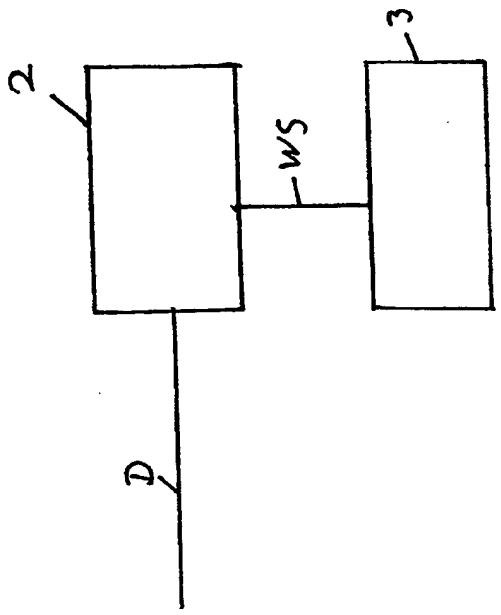


Fig. 3